

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

-----X

GARY TATINTSIAN, et al.,

Plaintiff, Counterclaim-Defendant,

-against-

Case No. 1:16-cv-7203-GHW

MIKHAIL VOROTYNTSEV, et al.,

Defendants, Counterclaim-Plaintiff, :

-----X

DMITRIY KHMALADZE and IT ADAPTER

CORPORATION INC.,

Plaintiffs, Counterclaim-Defendants,

-against-

Case No. 1:16-cv-8029-GHW

MIKHAIL VOROTYNTSEV, et al.,

Defendants, Counterclaim-Plaintiffs. :

-----X

INTELLIGENCE & PROSECUTION MEMORANDUM

**SUBJECT: THE CHEPA-TKACHEV-ISAEV-TATINTSIAN TRANSNATIONAL
CRIMINAL ORGANIZATION AND THE HOSTILE TAKEOVER OF SHOPLINK, INC.**

I. EXECUTIVE SUMMARY: ANATOMY OF A STATE-SPONSORED ASSAULT ON U.S. SOVEREIGNTY

This memorandum provides a comprehensive intelligence and legal analysis of a sophisticated, state-sponsored transnational criminal organization, hereafter "the Enterprise," led by sanctioned Russian State Duma Deputy Alexey Chepa and operating under the protection of General Ivan Tkachev, head of Russia's FSB Directorate K. The analysis establishes beyond a reasonable doubt that this Enterprise has engaged in a multi-year pattern of racketeering activity, the central objective of which was the hostile takeover of a U.S. technology company, ShopLink, Inc., and financial decimation of its founder, Mikhail Vorotyntsev. The ultimate goal was to convert this American company into a high-capacity, seemingly legitimate vehicle for laundering over \$100 billion in illicit funds.

The Enterprise's primary methodology has been the systematic corruption and weaponization of the United States judicial system. The litigations initiated in the U.S. District Court for the Southern District of New York (SDNY) are not legitimate commercial disputes but are, in fact, predicate acts of racketeering. These actions were meticulously orchestrated to financially decimate the victims, seize their company and intellectual property, and perpetrate a profound "fraud on the court." This assault was enabled by the active complicity of U.S.-based legal counsel who functioned as facilitators of the criminal scheme.

The key findings of this report are as follows:

- The Enterprise constitutes a structured criminal organization under the Racketeer Influenced and Corrupt Organizations (RICO) Act, engaging in a clear pattern of racketeering activity including wire fraud, money laundering, obstruction of justice, and extortion.
- The Enterprise's actions represent a direct and hostile attack on the sovereignty of the U.S. judicial system, constituting a significant national security threat. By co-opting the authority of a U.S. federal court, the Enterprise cloaked its private criminal acts in the power of the American state, a phenomenon analyzed herein as "Double State Coloring."
- This co-option of state power gives rise to constitutional violations, specifically the deprivation of property and liberty without due process, actionable under 42 U.S.C. § 1983.

This memorandum concludes with formal recommendations for immediate action. These include an urgent criminal referral to the United States Attorney for the Southern District of New York for the prosecution of all Enterprise members and facilitators under the RICO Act and other relevant federal statutes. Furthermore, it recommends decisive judicial action,

including the immediate stay of all related proceedings, the vacation of all judgments tainted by fraud pursuant to Fed. R. Civ. P. 60(b), the disqualification of complicit counsel, and the imposition of severe financial sanctions to protect the integrity of the American judicial process.

II. THE ENTERPRISE: COMMAND, MOTIVE, AND MODUS OPERANDI

To comprehend the attack on ShopLink, it is essential to first deconstruct the criminal organization that perpetrated it. The Enterprise is not a conventional criminal syndicate but a sophisticated hybrid organization that merges state power, political influence, legitimate business fronts, and criminal enforcement. Its actions are not random but are driven by a clear motive and executed according to a refined and repeatable playbook.

Section 2.1: Command and Control: The Tkachev-Chepa Axis

The Enterprise operates under a disciplined, top-down hierarchy that flows from the highest echelons of the Russian state security apparatus to operatives on the ground in the United States. This structure allows it to project power across international borders, leveraging state authority for protection in Russia and the U.S. legal system for offensive action abroad. This fusion of state and criminal elements represents a departure from traditional organized crime, functioning instead as a model for asymmetric conflict where the institutions of a target nation are turned against it.

- **The Apex Protector / "Krysha": General Ivan Tkachev.** As the head of the FSB's Directorate K, the counterintelligence arm for Russia's entire financial sector, General Tkachev provides the indispensable state protection, or "krysha" (roof), that makes the Enterprise's large-scale financial crimes possible.¹ His role is not passive protection but active collusion. This is proven conclusively by the aftermath of the BRT Bank collapse, a massive fraud that his directorate was mandated to investigate and prosecute. Instead, the state's 1.6 billion ruble claim against the bank's owners was diverted to a shell company secretly controlled by the primary perpetrator, Alexey Chepa—an inversion of justice impossible without Tkachev's facilitation.¹ His authority also enables the weaponization of the Russian state against the Enterprise's targets, as evidenced by the detention of Elena Vorotyntseva by Russian Customs and the subsequent quashing of the criminal investigation into the devastating gas explosion at her Moscow apartment, perpetrated by an intimidated housekeeper.¹
- **The Boss / Financial Architect: Alexey Chepa.** A sanctioned member of the Russian State Duma, Alexey Chepa serves as the Enterprise's operational commander and financial mastermind.¹ He orchestrated the ShopLink plot as a direct response to the collapse of his prior money laundering vehicle, BRT Bank.¹ He directs the U.S. operations and utilizes a network of family members, including his son Daniil Chepa,

daughter Anastasia Chepa, and niece Vera Afanasieva, to hold and conceal assets internationally, a hallmark of sophisticated financial crime.¹

- U.S. Operations Chief: Andrei Isaev.** As Chepa's chief lieutenant in the United States, Andrei Isaev is responsible for managing the hostile takeover on the ground.¹ He uses his Tanuki restaurant chain, a cash-intensive business, as both a financial front and an operational base.¹ His primary value to the Enterprise is his documented history of 154 predatory litigation cases, making him the designated enforcer for the Enterprise's playbook of lawfare in the U.S..¹
- U.S. Field Agent / Enforcer: Gary Tatintsian (GT).** Acting as Isaev's "foot soldier," GT was responsible for identifying and infiltrating ShopLink.¹ He initiated the fraudulent litigation that served as the primary weapon of the takeover and used his New York art gallery as an operational hub and a front, which acts as a conduit for laundering funds.¹ The high-end art market's opacity and lack of regulation make it an ideal environment for such activities.¹
- Financial Architects / Field Managers: Alexander Sysoev & Vladimir Mukhin.** These key partners of Chepa were co-owners of BRT Bank, placing them at the core of the Enterprise's Russian financial operations.¹ They serve as the critical bridge between the Russian financial wing and the U.S. lawfare operations. They provide the financial instruments, such as debt claims, that are weaponized to create a pretext for predatory lawsuits, a tactic proven in the 'Krispy Kreme' case.¹

Table 1: Enterprise Key Personnel and Roles

Individual	Primary Affiliation	Role in Enterprise	Key Actions in ShopLink Plot
Ivan Tkachev	Head, FSB Directorate K	The Apex Protector / "Krysha"	Provides state-level protection for financial crimes; enables weaponization of Russian state apparatus (e.g., customs arrest of EV). ¹
Alexey Chepa	Sanctioned Russian State Duma Deputy	The Boss / Financial Architect	Masterminded the ShopLink plot after BRT Bank collapse; directs U.S. operations; uses family to conceal assets. ¹

Andrei Isaev	Founder, Tanuki Restaurants	U.S. Operations Chief	Manages U.S. operations and fronts; specialist in predatory litigation; orchestrates sham lawsuits to create smokescreens. ¹
Gary Tatintsian (GT)	Owner, Tatintsian Gallery	U.S. Field Agent / Enforcer	Identified and infiltrated ShopLink; initiated fraudulent litigation; used gallery as operational hub and money laundering front. ¹
Alexander Sysoev	Co-owner, BRT Bank	Financial Architect	Co-managed BRT Bank money laundering; provided financial instruments for predatory litigation. ¹
Vladimir Mukhin	Co-owner, BRT Bank	Financial Architect	Co-managed BRT Bank; critically, assigned his debt claim to Isaev to manufacture legal standing for the 'Krispy Kreme' lawsuit. ¹
Dmitriy Khmaladze (DK)	Former ShopLink CTO	Insider Threat	Committed systematic perjury to steal IP; provided the fraudulent basis for the collusive <i>Khmaladze</i> lawsuit. ¹
Younis Zubchevich (YZ)	Former Advisor to MV	The Betrayer / Coordinator	Breached trust to coordinate the takeover; facilitated witness tampering and spread disinformation to investors. ¹
Chepa Family Network	Family Members	Asset Holders	Used to conceal beneficial ownership

			of illicitly acquired assets across jurisdictions (e.g., London, Miami). ¹
--	--	--	---

Section 2.2: The Catalyst: The Collapse of BRT Bank

The plot against ShopLink was not arbitrary; it was born of a specific and urgent crisis. On May 27, 2016, the Central Bank of the Russian Federation revoked the banking license of the Commercial Bank "Bank for Development of Technologies" (BRT).¹ The state regulator cited systemic criminal activity, including failure to comply with laws on "countering the legalisation (laundering) of criminally obtained incomes" and the creation of a massive hole in the bank's balance sheet from asset stripping.¹

This event was a catastrophic blow to the Enterprise. BRT Bank, controlled by Chepa with Sysoev and Mukhin as key partners, was their primary engine for washing and moving illicit funds.¹ Its collapse left the Enterprise's leadership facing a 1.6 billion ruble liability to the state's Deposit Insurance Agency and, more critically, without a functioning large-scale laundering mechanism.¹

This desperation was the direct catalyst for the ShopLink conspiracy. The Enterprise urgently needed a new vehicle, but one more sophisticated than a traditional bank. A "hot US tech company" offered the perfect solution. The narrative of explosive growth and high valuation could plausibly explain the injection of hundreds of millions, or even billions, of dollars in sham "investment" rounds.¹ This motive is corroborated by GT's secretly recorded meeting on April 8, 2016—before the bank's collapse but as the enterprise was clearly planning for contingencies—where he forcefully extracted a promise from MV that ShopLink would not be sold for less than \$100 billion. This was not a business negotiation; it was the creation of a public relations "deliverable" to justify the future mega-funding rounds that would be used to legitimize the Enterprise's dirty money.¹

Section 2.3: The Playbook: Precedents in Predatory Lawfare

The methods used against ShopLink were not improvised but were the U.S. deployment of a codified and repeatable criminal playbook honed in Russia. Prior cases involving the Enterprise's key members serve as proof of concept, establishing a clear *modus operandi*. The existence of this playbook elevates the ShopLink attack from a singular crime to an act of a continuing criminal enterprise, a core element for RICO prosecution.

- **The 'Taras Bulba' Precedent:** This case demonstrates the Enterprise's capacity for

selective weaponization of state power. The founder of the "Taras Bulba" restaurant chain, Yuri Beloyvan, was a business partner of Andrei Isaev, who held a 34% stake.¹ Starting around 2016, Beloyvan was systematically destroyed by a multi-year, multi-agency assault by Russian authorities, including a massive tax prosecution, imprisonment, and eventual bankruptcy, forcing him to flee the country.¹ Throughout this campaign, his partner, Andrei Isaev, remained completely untouched.¹ This starkly contrasts with a 2011 tax evasion case against Isaev's own Tanuki chain, where the investigation was contained and a lone manager was made the scapegoat, shielding the owners.¹ The differential outcomes prove a pattern: state power is deployed with maximum force to eliminate an external partner, but it is neutralized to protect the Enterprise's own assets and leadership.

- **The 'Krispy Kreme' Precedent:** This case demonstrates the Enterprise's mastery of using civil litigation as an offensive weapon. The Russian Krispy Kreme franchise was a joint venture between famed restaurateur Arkady Novikov and Enterprise members Alexander Sysoev and Vladimir Mukhin.¹ To fund expansion, Sysoev and Mukhin provided loans to the venture.¹ Years later, when the Enterprise decided to move against Novikov, it executed a key legal maneuver: Vladimir Mukhin assigned his debt claim to Andrei Isaev, who was not an original party to the loan.¹ This was a calculated act of lawfare. It armed Isaev, the Enterprise's designated legal enforcer, with the legal standing necessary to launch a predatory lawsuit against his own business partner. This establishes the playbook of acquiring or assigning debt claims for the specific purpose of manufacturing a legal dispute and attacking a target through the civil courts.

- **The Ultimate Power Play: The Diversion of the 1.6 Billion Ruble State Claim via 'Prommashekspo-1'**

The most audacious and revealing act undertaken by the Chepa-Tkachev enterprise is the diversion of the 1.6 billion ruble state claim stemming from the BRT Bank collapse. This maneuver represents the pinnacle of state capture and provides the most direct evidence of General Ivan Tkachev's active collusion in the enterprise's criminal activities.

Following the 2016 revocation of BRT Bank's license, the Russian state, through its Deposit Insurance Agency (DIA), was left with a 1.6 billion ruble claim against the bank's owners - Alexey Chepa, Alexander Sysoev, and Vladimir Mukhin - for the funds needed to repay insured depositors.³ The DIA is a state corporation tasked with recovering such funds through legal action against the responsible parties. Instead of pursuing this claim, the DIA engaged in an act that defies all legal and commercial logic: it transferred the entirety of its 1.6 billion ruble claim to an obscure private entity, ООО "Проммашэкспо-1" (Prommashekspo-1).³ Russian arbitration court records confirm that in April 2021, Prommashekspo-1 initiated legal proceedings to

recover these "damages" from the former managers of BRT Bank, having become the legal successor to the state's claim.²⁸

This transfer was a sham designed to shield Alexey Chepa from his liability to the state. Analysis of Russian corporate and banking registries proves conclusively that Prommashekspo-1 is a shell company within Chepa's own network of controlled entities. The most definitive piece of evidence is a 2016 disclosure from BRT Bank itself, which lists the entities under Chepa's control. It explicitly states that Prommashekspo-1 "forms a group of persons" with Chepa, who "is the person under whose control and significant influence... the bank is located".⁸ Further corporate records show Chepa as an indirect founder of Prommashekspo-1 through a web of other companies he controls, such as "VITA M+" and "S.K. Accord".³¹

The significance of this cannot be overstated. Alexey Chepa, the debtor who owed the Russian state 1.6 billion rubles, orchestrated a scheme whereby the state's legal claim against him was transferred to his own secret company. He effectively became his own creditor, erasing the debt and laundering the proceeds of his bank's fraudulent collapse with the active participation of the state agency meant to be pursuing him.

This act of profound corruption is impossible without protection from the highest levels of Russia's security apparatus. The financial sector, and particularly the activities of the state Deposit Insurance Agency, falls squarely within the jurisdiction of the FSB's Directorate K. For the DIA to execute such a transfer, which is facially contrary to the state's interests, it would require, at minimum, the acquiescence of General Ivan Tkachev. More plausibly, it required his active direction. This maneuver is the enterprise's masterstroke, demonstrating a level of control over the Russian state that elevates this conspiracy far beyond ordinary organized crime and into the realm of a state-integrated criminal syndicate.

III. THE SHOPLINK CONSPIRACY: A CHRONOLOGICAL DECONSTRUCTION

The assault on ShopLink unfolded in four distinct but interconnected phases. The timeline reveals a clear, causal chain of escalation, where each act of resistance by the victim, Mikhail Vorotyntsev, was met with a disproportionately hostile and criminal counter-move by the Enterprise. This reactive escalation demonstrates that the Enterprise's goal was never the resolution of a legitimate dispute but total subjugation and asset seizure.

Section 3.1: Phase I - Infiltration and Intelligence Gathering (Oct 2015 - Apr 2016)

The operation began with a classic intelligence-gathering and infiltration campaign designed to assess the target's value and vulnerabilities.

- **October 2015:** Gary Tatintsian (GT) initiated contact with ShopLink. He conducted secret audio recordings of meetings at the law firm Pryor Cashman, gathering detailed intelligence on ShopLink's corporate structure and governance weaknesses.¹ To build trust and gain deeper access, he executed a strategic maneuver: wiring \$250,000 to ShopLink without formal documentation, only to withdraw the investment days later after his intelligence objectives were met.¹
- **December 2015:** The Enterprise's future insider threat, ShopLink's CTO Dmitriy Khmaladze (DK), agreed via Skype to a four-year vesting schedule for his compensation, a material fact he would later deny under oath.¹
- **April 8, 2016:** GT re-engaged as an investor, this time setting an entrapment. In another secretly recorded meeting, he manipulated the subscription agreement and, most critically, extracted from MV the "\$100 Billion" valuation narrative. This was not a good-faith investment term but a premeditated effort to create a plausible public cover story for the massive money laundering operation his Russian superiors were planning.¹

Section 3.2: Phase II - Motive & Declaration of War (May - Aug 2016)

This phase marks the emergence of the definitive motive and the explicit shift from infiltration to hostility.

- **May 27, 2016 (THE MOTIVE):** The Enterprise's primary money laundering vehicle, BRT Bank, had its license revoked by the Russian Central Bank, creating an urgent, existential need for a new mechanism.¹
- **May - August 2016:** In the immediate aftermath of the bank's collapse, a significant flow of operational funds is observed. Approximately \$10 million was wired from Pelican Ventures LLC, an entity linked to Andrei Isaev, to GT's art gallery. This capital was designated to finance the hostile takeover and subsequent sham litigations.¹
- **July 23, 2016:** GT received confirmation from Pryor Cashman that his investment was "locked in" and Shoplink had no rescission rights, solidifying GT's position within the company and setting the stage for a hostile, rather than purely financial, strategy.¹
- **August 19, 2016 (THE TRIGGER):** The conspiracy was irrevocably set on a hostile path when MV informed GT of a potential partnership with KKR, a premier U.S. private equity firm.¹ A legitimate institutional investor like KKR would subject ShopLink to rigorous due diligence, transparency, and governance standards, making the Enterprise's money laundering scheme impossible. This posed a mortal threat to the entire criminal plot.
- **August 23, 2016:** GT's reaction was immediate and violent. He sent a "declaration of war" email, explicitly rejecting any buyout and threatening to crush MV with overwhelming litigation, boasting, "I can afford much more to sped to fighting u then you all!!".¹ This was coupled with threats of physical violence, including dissolving MV

and Elena Vorotyntseva ("EV") in acid.

- **Aug 26-27, 2016:** YZ mediates a meeting between GT and MV, in NYC, during which GT becomes violent and threatens MV's life. The following day YZ sends a conciliatory email "Getting Consensus" to GT and MV, in which he lays out a 14 point plan on how to proceed with Shoplink corporate governance clean up and inaugural launch, GT replies "sounds like a plan. Agreed" and MV reluctantly agrees, but states that GT shocked him with promises to "destroy Shoplink, simply because he can".
- **Aug 30, 2016:** GT sends a threat letter to MV, from YZ's lawyer Nussbaum, demanding Shoplink Board control.
- **Aug 31, 2016:** DK secretly deletes Shoplink source code files from Gdrive, after a long conversation with GT.

Section 3.3: Phase III - The "Smash-and-Grab" & Court Weaponization (Aug/Sep 2016 - Mar 2017)

With war declared, the Enterprise executed a swift, multi-pronged "smash-and-grab" operation to seize the company's assets and weaponize the U.S. courts to legitimize the theft.

- **September 1, 2016:** Co-conspirator Younis Zubchevich (YZ), MV's former advisor, circulated the hostile takeover plan to DK and GT, the U.S. operational cell.¹
- **Sep 6, 2016:** GT and DK meet in OH, GT sends an email to DK stating that he saw in Shoplink: "incredible opportunity and wanted to help with financing and structuring it".
- **September 8, 2016:** The corporate vehicle for the stolen assets, Agnicore LLC, was secretly formed by the conspirators.¹
- **September 11, 2016:** GT emailed DK a legal analysis on how to breach his contracts with MV. On the same day, DK resigned from ShopLink, poached the entire development team, and seized control of the company's source code repositories, effectively decapitating the company's technical operations.¹
- **September 15, 2016:** GT filed the primary fraudulent lawsuit, *Tatintsian v. Vorotyntsev*, and procured a Temporary Restraining Order (TRO), paralyzing ShopLink's ability to operate or seek funding.¹
- **October 13, 2016:** DK filed his collusive and perjurious lawsuit, *Khmaladze v. Vorotyntsev*, to create the fraudulent legal predicate for the intellectual property theft.¹
- **December 1, 2016:** DK executed the "classic intellectual property misappropriation," filing a fraudulent patent application on behalf of Agnicore that removed MV as the original inventor and transferred ShopLink's core IP to the Enterprise's shell company.¹
- **December 7, 2016:** The Enterprise began to weaponize other government agencies. GT and YZ orchestrated the fraudulent inducement of an investigation by the New York

Attorney General's (NYAG) office, intending to use it as leverage against MV and to intimidate other investors into joining their cause.¹

- **March 1, 2017:** In a preemptive strike designed to control the narrative and intimidate key third-party witnesses, GT filed a fraudulent lawsuit against ShopLink's own corporate law firm, Pryor Cashman.¹

Section 3.4: Phase IV - Transnational Warfare and Intimidation (2017 - Present)

When the initial legal assault failed to secure a quick victory, the Enterprise escalated its tactics to a campaign of transnational warfare, demonstrating its global reach and willingness to use extra-judicial methods.

- **October - December 2017:** GT and YZ engaged in direct economic sabotage, successfully destroying major business deals ShopLink had secured with Shea Moisture and with Hillary Clinton's publisher by contacting the counterparties and falsely claiming MV was under federal criminal investigation.¹ Simultaneously, they issued explicit death threats against MV and his wife, Elena Vorotyntseva (EV), to the CEO of MV's new business venture, MovieCoin, causing that partnership to collapse.¹
- **June 2018 - Ongoing:** The financial warfare expanded internationally. The Enterprise instigated fraudulent Suspicious Activity Reports (SARs) and investigations to freeze millions of dollars of the victims' personal and corporate assets in London and the European Union, a clear strategy to cripple their ability to fund a legal defense.¹
- **August 2021:** The Enterprise leveraged its state power in Russia directly. EV was detained by Russian Customs—an agency within FSB General Tkachev's sphere of influence—while traveling for medical treatment. The arrest, for allegedly "smuggling" her own jewelry, was a transparent act of state-sponsored intimidation.¹
- **September 2022:** The intimidation escalated to physical violence with a devastating gas explosion at EV's Moscow apartment. The subsequent criminal investigation in Russia was abruptly "squashed" by a "very powerful" figure, pointing directly to Tkachev's protective "krysha".¹
- **August 2023:** To create a smokescreen and conceal the ongoing conspiracy from the SDNY court, the Enterprise staged a collusive, sham lawsuit, *Isaev v. Tatintsian*. This legal theater was designed to create a false record of animosity between the key U.S. operatives and to provide a court-sanctioned channel for laundering operational funds.¹

IV. THE CRIME SCENE: FRAUD ON THE COURT AND THE CORRUPTION OF U.S. JUSTICE

The core of the Enterprise's U.S. operation was not the theft of intellectual property, but the corruption of the judicial process used to legitimize that theft. The SDNY courtroom was

not a forum for dispute resolution; it was the designated crime scene. The Enterprise perpetrated a profound "fraud on the court," which is not merely a wrong against an opposing party, but a public wrong against the institution of justice itself. This fraud was systematic, multifaceted, and designed to be procedurally undiscoverable through the normal channels of litigation, thereby attacking the very machinery of justice.

Section 4.1: The Three Pillars of Perjury

The collusive lawsuit, *Khmaladze v. Vorotyntsev*, was built on a foundation of three distinct, material, and deliberate acts of perjury by Dmitriy Khmaladze. These falsehoods were engineered to create a completely fabricated factual predicate upon which the court would unknowingly base its rulings.

- **The R7 Software Ownership Fraud:** The entire premise of DK's lawsuit rested on his sworn assertion in his complaint that a software program he termed "R7" was his own independent creation, developed prior to his work with ShopLink.¹ This was a calculated lie. Overwhelming evidence, including DK's own deposition testimony and internal ShopLink technical documents that he personally authored, proves that "R7" was merely an internal codename for ShopLink's proprietary source code.¹ As the company's CTO, DK's misrepresentation was not a simple factual error but a deliberate "technical fraud" from a subject matter expert, designed to mislead the court on the central issue of intellectual property ownership.¹
- **The Patent Inventorship Theft:** On December 1, 2016, DK filed a patent application on behalf of the newly formed shell company, Agnicore LLC. This filing fraudulently removed Mikhail Vorotyntsev as the original inventor from ShopLink's pre-existing patent applications and transferred the intellectual property rights to the Enterprise's new entity.¹ This was an act of "classic intellectual property misappropriation," committed despite DK's clear knowledge of MV's inventorship from prior patent filings.¹
- **The Rule 56.1 Perjury:** The pattern of deceit continued into the dispositive motions phase of the litigation. In a sworn Local Rule 56.1 Statement filed on April 22, 2022, DK stated under penalty of perjury that "No evidence has been produced by any party showing that Defendants' intellectual property was misappropriated by Khmaladze".¹ This statement was demonstrably false when made. The most direct and irrefutable evidence of the misappropriation was DK's own fraudulent patent filing from 2016. This perjury, in a document intended to guide the court's factual findings for summary judgment, was a direct attempt to corrupt the judicial process at a crucial stage.¹

Section 4.2: The Settlement Confession: An Admission of Fraudulent Inception

The most damning proof of the lawsuit's entirely fabricated nature comes from the

Enterprise's own legal representatives. On May 13, 2019, during settlement negotiations, counsel for Dmitriy Khmaladze relayed a formal offer to ShopLink's counsel.¹ The offer stated that DK was prepared to "give up his claims and walk away entirely" and, critically, that he was "no longer challenging the validity of any contracts".¹

This communication is not a routine settlement posture; it is a direct and unambiguous contradiction of every material allegation in DK's sworn complaint, which was predicated entirely on the claim that the contracts were invalid and that he, not ShopLink, owned the intellectual property. This offer, conveyed by an agent of the party, constitutes an admission that the entire lawsuit was a sham from its inception. It reveals that the Enterprise pursued claims it knew were meritless, weaponizing the cost and burden of federal litigation as a tool of extortion, hoping to force a settlement from a victim it was simultaneously crippling through other means.¹

Section 4.3: Systematic Obstruction and Spoliation

The Enterprise's fraud was not limited to false statements; it included a coordinated campaign to actively destroy and conceal the very evidence that would have exposed the lies. This conduct demonstrates a consciousness of guilt and was designed to make the truth procedurally undiscoverable, thereby incapacitating the victims and deceiving the court.

Immediately upon his resignation on September 11, 2016, and just before the lawsuits were filed, DK took decisive steps to spoliage evidence. He blocked MV's access to all of ShopLink's source code repositories and, three days later, blocked access to corporate email accounts.¹ Evidence indicates that he had already "deleted most incriminating emails before his resignation".¹

These were not the actions of a party engaged in a legitimate dispute. They were the actions of a saboteur preemptively destroying the evidence of his crime. This systematic obstruction directly prevented the victims from achieving "full factual development" during discovery and was a primary contributor to their inability to uncover the full extent of the perjury earlier in the litigation.¹ Such conduct is a quintessential hallmark of extrinsic "fraud on the court," as it is an attack on the judicial machinery itself, designed to prevent a fair adversarial contest. This is precisely why any defense based on the victim's supposed "lack of diligence" is legally and factually untenable. To reward the perpetrator for the efficacy of their own cover-up would create a perverse incentive and contravene the Supreme Court's controlling precedent in *Hazel-Atlas Glass Co. v. Hartford-Empire Co.*, which holds that the preservation of judicial integrity cannot wait upon the diligence of litigants when the court itself has been defrauded.¹

V. LEGAL ANALYSIS: A PATTERN OF RACKETEERING AND CONSTITUTIONAL VIOLATIONS

The factual record establishes a compelling basis for prosecution under multiple federal statutes. The Enterprise's coordinated actions constitute a classic pattern of racketeering activity, and its method of co-opting state power gives rise to profound constitutional violations.

Section 5.1: Racketeer Influenced and Corrupt Organizations (RICO) Act Violations (18 U.S.C. §§ 1961-1968)

The Enterprise's conduct falls squarely within the ambit of the RICO Act. The organization, comprising a clear hierarchy and a group of individuals associated in fact to pursue a common criminal purpose, constitutes an "enterprise" as defined in 18 U.S.C. § 1961(4). This Enterprise engaged in a clear "pattern of racketeering activity" through the commission of numerous, interrelated predicate offenses over a period of nearly a decade.

Table 2: Analysis of RICO Predicate Acts

Predicate Act	U.S. Code Section	Specific Action by Enterprise	Key Personnel	Evidentiary Support
Wire Fraud	18 U.S.C. § 1343	Electronic filing of fraudulent lawsuits (<i>Tatintsian, Khmaladze, Isaev</i>) via the interstate ECF system to execute a scheme to defraud.	GT, DK, Isaev, Counsel	¹
Obstruction of Justice	18 U.S.C. §§ 1503, 1512	Filing of perjurious complaints and affidavits (DK); systematic witness tampering (GT/YZ maligning MV to investors); filing	DK, GT, YZ, Isaev	¹

		of the collusive <i>Isaev</i> lawsuit to mislead the court.		
Money Laundering	18 U.S.C. § 1956	Transfer of \$10M from Pelican Ventures to GT's gallery; use of the <i>Isaev v. Tatintsian</i> settlement to transfer over \$2M between co-conspirators to conceal and promote unlawful activity.	Isaev, GT	¹
Extortion (Hobbs Act)	18 U.S.C. § 1951	GT's threats of "financial warfare" and physical violence (death threats, "dissolve... in acid") to obtain property (ShopLink shares and control) from MV.	GT	¹
Interstate Transportation of Stolen Property	18 U.S.C. § 2314	The fraudulent transfer of ShopLink's intellectual property (software, patent rights), valued at over \$5,000, to Agnicore LLC, an entity controlled by conspirators across state lines.	DK, GT, YZ	¹

Section 5.2: The "Double State Coloring" Doctrine and 42 U.S.C. § 1983 Claims

The Enterprise's methodology triggers liability under 42 U.S.C. § 1983 for the deprivation of constitutional rights. While the primary conspirators are private actors, their conduct satisfies the "state action" requirement through a novel legal framework designated here as "Double State Coloring."

- **First-Layer State Coloring (The Foreign Sovereign Shield):** The Enterprise's leadership by senior Russian officials (Chepa and Tkachev) provides the initial layer of state coloring. This foreign state backing shields their transnational crimes and enables acts of sovereign power, such as the asset freezes in Europe and the detention of EV by Russian Customs, which are used to intimidate and incapacitate their U.S. target.¹
- **Second-Layer State Coloring (The U.S. State Sword):** The Enterprise then weaponized its resources to co-opt the machinery of the U.S. government itself. By perpetrating a systematic fraud on the SDNY and fraudulently inducing an investigation by the NYAG, the Enterprise converted the authority of these American institutions into a second layer of state coloring.¹ The court's own orders—the TROs, discovery mandates, and summary judgments—became the instruments of the racketeering scheme, cloaking private criminal acts with the authority of the U.S. state.¹

This conduct satisfies the "state action" requirement under established legal tests. By maliciously conspiring to deceive the court and use its coercive power to deprive the victims of their property, the private actors became "willful participant[s] in joint action with the State or its agents".¹ The court, rendered an unwitting instrument by the fraud, becomes the state actor whose power is abused. This systematic corruption of the judicial process resulted in a profound deprivation of the victims' property (ShopLink, its IP, personal assets) and liberty interests without the procedural due process guaranteed by the Fifth and Fourteenth Amendments.¹

Section 5.3: Financial Crimes and Transnational Warfare

The financial component of the conspiracy was sophisticated and served two primary purposes: financing the U.S. legal assault and laundering the proceeds of the Enterprise's broader activities. A detailed financial trace reveals two key transactions:

1. **The Pelican Ventures Funding:** Between May and August 2016, immediately following the BRT Bank collapse, \$9.95 million was wired from Pelican Ventures LLC (an entity where Isaev acted as an agent) to GT's gallery.¹ This transaction, disguised as a payment for art, was in fact the seed capital used to finance the "sham litigations" against MV and ShopLink.¹
2. **The Isaev v. Tatintsian Laundering:** The 2023 sham lawsuit between Isaev and GT culminated in a court-recognized settlement requiring GT to pay Isaev over \$2 million.¹ This settlement was not a resolution of a real dispute but a mechanism to launder

operational funds, creating a legitimate legal pretext for a large financial transfer between the Enterprise's U.S. chief and his primary field agent.¹

This financial warfare was complemented by a campaign of direct economic sabotage. The Enterprise successfully destroyed lucrative business deals with Shea Moisture, MovieCoin and Hillary Clinton's publisher by making false claims of criminal investigations to those counterparties.¹ Furthermore, they initiated fraudulent SARs and legal proceedings in London and the EU to freeze millions of dollars in the victims' assets, a clear strategy to deny them the resources needed to mount a legal defense.¹

VI. THE FACILITATORS: COMPLICITY OF OFFICERS OF THE COURT

The Enterprise's assault on the U.S. judiciary could not have succeeded without the active participation of U.S.-based legal counsel. The evidence indicates that these officers of the court - including Kristen Santillo, Partha Chatteraj, Robert Pittman, and Lawrence Nussbaum transcended the role of zealous advocates and became willful facilitators of the criminal conspiracy. Their involvement was not merely an ethical lapse; it was a critical operational component that provided the procedural knowledge and veneer of legitimacy necessary to weaponize the U.S. legal system.

Section 6.1: A Pattern of Ethical and Legal Breaches

The conduct of the Enterprise's counsel demonstrates a pattern of severe breaches of the ABA Model Rules of Professional Conduct, transforming them from advocates into co-conspirators.

- **Violation of Rule 3.3 (Candor Toward the Tribunal):** Counsel repeatedly presented documents to the court that they knew or should have known contained perjured statements. This includes Partha Chatteraj filing DK's initial complaint, which was founded on the "R7 software" lie, and the subsequent filing of the false Rule 56.1 statement.¹ Their failure to correct these material falsehoods, especially after the "settlement confession" revealed the claims were baseless, constitutes a profound breach of their duty of candor.¹
- **Violation of Rule 3.4 (Fairness to Opposing Party and Counsel):** Counsel enabled, assisted in, or failed to prevent their clients' systematic obstruction of justice. This includes DK's spoliation of evidence (deleting emails, blocking code access) and the campaign of witness tampering and intimidation directed at ShopLink's other investors and business partners.¹
- **Violation of Rule 1.2(d) (Counseling or Assisting Client in Criminal or Fraudulent Conduct):** Counsel's role went beyond advocacy to active assistance in criminal acts. This is evidenced by their facilitation of the fraudulent patent filing that constituted intellectual property theft and by providing "legal analysis" on how DK could breach

his contracts in furtherance of the "smash-and-grab" scheme.¹

Section 6.2: The "Santillo Connection" and the Crime-Fraud Exception

The most direct evidence of counsel's integration into the conspiracy is the "Santillo Connection." A text message from co-conspirator Younis Zubchevich regarding GT's counsel, Kristen Santillo, stated, "She will rep me if I'm served".¹

This statement is not an innocuous inquiry about representation. It is evidence that counsel was "pre-positioned" to represent multiple members of the criminal cell as part of a coordinated legal strategy. It suggests that the attorney-client relationship was being used not for legitimate defense, but as a shield to coordinate the activities of the conspiracy and conceal its communications. This abuse of the attorney-client privilege to plan and facilitate a "hybrid criminal-civil conspiracy" is a perversion of legal ethics.¹

This conduct directly triggers the crime-fraud exception to attorney-client privilege. When there is probable cause to believe that legal advice was sought or obtained in furtherance of ongoing or future criminal or fraudulent activity, the privilege is defeated.¹ The evidence of counsel's pre-positioning and their role in facilitating the fraud on the court provides a sufficient basis to pierce the privilege and investigate the full extent of their communications with the Enterprise's members regarding the planning and execution of the conspiracy.

VII. CONCLUSION AND RECOMMENDATIONS

The totality of the evidence presents a coherent, undeniable, and deeply disturbing narrative. A transnational criminal organization, sponsored and protected by senior officials of the Russian Federation, has systematically infiltrated and weaponized the U.S. judicial system. This was not a business dispute that devolved into aggressive litigation; it was a premeditated criminal campaign to commit a hostile takeover and convert a U.S. company into a global money laundering vehicle.

Section 7.1: Finding of Fact: A Hostile Attack on U.S. Judicial Sovereignty

It is the definitive finding of this analysis that the actions of the Chepa-Tkachev-Isaev-Tatintsian Enterprise constitute a direct and hostile assault on the sovereignty and integrity of the United States judiciary. A foreign criminal network, inextricably linked to the intelligence services of a geopolitical adversary, has deliberately corrupted a United States District Court, transforming it from a forum for justice into an instrument of racketeering. They have filed fraudulent lawsuits, submitted perjured testimony, and engaged in collusive legal theater with the express purpose of deceiving a

federal judge. This is not litigation; it is information warfare conducted within the sanctuary of the American legal system. To permit the results of this corruption to stand would be to concede that a U.S. court can be successfully subverted by a hostile foreign criminal enterprise, an outcome with grave implications for the rule of law and national security.

Section 7.2: Recommendations for Criminal Referral

Based on the comprehensive evidence establishing probable cause for multiple federal crimes, it is formally and urgently recommended that the Court make an immediate criminal referral to the United States Attorney for the Southern District of New York. A grand jury investigation should be initiated into the Chepa-Tkachev-Isaev-Tatintsian Enterprise and all its identified members and facilitators.

The referral should recommend pursuing charges including, but not limited to:

- **Violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act (18 U.S.C. § 1962(c) and (d)):** Against all core members of the Enterprise for conducting and conspiring to conduct the affairs of an enterprise through a pattern of racketeering activity.
- **Wire Fraud (18 U.S.C. § 1343):** For the use of the court's electronic filing system in furtherance of the scheme to defraud.
- **Obstruction of Justice (18 U.S.C. § 1512):** For corruptly impeding the due administration of justice through sham litigation, perjury, and witness tampering.
- **Money Laundering (18 U.S.C. § 1956):** For using financial transactions, including a court settlement, to conceal and promote the proceeds of unlawful activity.
- **Violations of U.S. Sanctions Laws (50 U.S.C. § 1705 - IEEPA):** For conducting transactions for the benefit of a sanctioned individual, Alexey Chepa.
- **Perjury (18 U.S.C. § 1621):** Against Dmitriy Khmaladze for his multiple false statements under oath.

Section 7.3: Recommendations for Judicial Action

To protect its own integrity and remedy the profound injustice perpetrated, it is recommended that the Court exercise its inherent authority to take the following immediate and decisive actions:

1. **Immediate Stay of All Proceedings:** All matters in *Tatintsian v. Vorotyntsev* (1:16-cv-7203-GHW) and *Khmaladze v. Vorotyntsev* (1:16-cv-8029-GHW) must be immediately stayed to halt the ongoing abuse of process.¹
2. **Vacation of All Tainted Judgments:** All prior judgments and orders procured through this systematic fraud must be vacated pursuant to Federal Rule of Civil Procedure 60(b)(3), 60(b)(6), and the Court's inherent power to remedy "fraud on the court,"

which is not subject to time limitations.¹

3. **Immediate Disqualification of Counsel:** Legal counsel for Gary Tatintsian and Dmitriy Khmaladze, and their respective firms, must be immediately disqualified from further representation for their role as active facilitators of the fraud on the Court.¹
4. **Imposition of Severe Financial Sanctions:** Substantial cash bonds of no less than \$1.5 million each must be imposed upon Gary Tatintsian, Dmitriy Khmaladze, and their respective legal counsel and firms. This is necessary to secure potential damages, deter further vexatious conduct, and ensure accountability for a nine-year campaign of financial warfare and asset manipulation.¹

The evidence trail is robust, the pattern of conduct is clear, and the criminal intent is palpable. The actions of this enterprise were not a mere business dispute gone wrong; they were a calculated assault by a sophisticated foreign criminal organization. It is within the power of the U.S. Department of Justice and the Southern District of New York to unmask these perpetrators, dismantle their U.S. operations, and defend the rule of law from this hostile foreign intrusion.

Respectfully submitted,

/s/Mikhail Vorotyntsev

Mikhail Vorotyntsev
Pro Se
Founder, ShopLink Inc.

Cc: All Counsel of Record

Citations:

1. Motion to Disqualify and Sanction Counsel - H_GHW.pdf